United Nations A/60/695

General Assembly

Distr.: General
24 February 2006

Original: English

Sixtieth session
Agenda item 124
Programme budget for the biennium 2006-2007

Strengthened and unified security management system for the United Nations: standardized access control

Report of the Secretary-General

Summary

The present interim report, issued pursuant to General Assembly resolution 59/294, outlines the proposed scope, concept and revised course of action for standardized access control at all main locations of the Organization. It also provides, for further consideration by the General Assembly, the additional information requested in section XI, paragraph 44, of its resolution 59/276, along with the estimated costs involved in addressing critical requirements that should be implemented without delay. The additional improvements identified will bring all main duty stations to a baseline security level with regard to control of access to United Nations premises. The report sets a new timetable for submission to the Assembly at its sixty-first session of a detailed plan for implementation of the project.

06-25340 (E) 030306

I. Introduction

1. The Secretary-General has proposed for implementation a number of projects to strengthen security and safety at United Nations facilities at Headquarters and other main locations (see A/58/756 and A/59/365/Add.1 and Corr.1). A global access control system, with the aim of ensuring full perimeter security through an integrated and coordinated approach that would allow system and information-sharing among all duty stations, was included among those proposals (A/59/365/Add.1, para. 26).

2. By section XI, paragraph 44, of its resolution 59/276, the General Assembly decided to defer until the second part of its resumed fifty-ninth session consideration of the specific project for a global access control system, pending receipt of a detailed report on the following issues:

(a) Integration with projects approved by the Assembly in previous resolutions, including those in the overall information technology strategy;

(b) The impact of implementing the global access control system on human resources requirements in the area of safety and security;

(c) The individual characteristics of each United Nations headquarters and main duty station;

(d) The implications of the global access control system for the capital master plan;

(e) Detailed information regarding the global identity management system, including the principles and guidelines for sharing the information obtained through the system, the level of centralization needed for managing the information and who would have access to the information;

(f) The time frame for implementation of the system.

3. The Secretary-General has determined that a standardized access control system at all main locations would require a high level of integration and coordination, with project management and delivery mechanisms defined from the inception of the project to ensure its ultimate success (see A/59/776). The Secretary-General therefore proposed that a project access control team be established within the Department of Safety and Security with the aim of planning and, in the event that the project is later approved, coordinating, in close consultation with the Office of Central Support Services, the implementation of a comprehensive, fully integrated and standardized access control system. He has further proposed that the project access control team would commence its work with a review of previous studies and earlier external validations of the project, carry out further studies as may be required and prepare a detailed preliminary design and cost analysis. The resulting standardized access control proposals were expected to include viable alternatives where possible, an assessment of their impact on achieving headquarters minimum operating security standards and measures to prevent cost overruns. A time frame of six to nine months was proposed for planning and preliminary design. The implementation phase was estimated to require 18 to 24 months, following approval of the project concept and design by the General Assembly.

4. The General Assembly, in its resolution 59/294, took note of the report of the Secretary-General (A/59/776) and endorsed the observations and recommendations

of the Advisory Committee on Administrative and Budgetary Questions (A/59/785), including the recommendation for submission of a comprehensive report on the project to be reviewed by the Assembly during its sixtieth session.

II. Proposed concept for standardized access control at United Nations facilities

A. General aspects

5. The aim of the standardized access control project is to ensure an appropriate level of physical security at the United Nations Headquarters premises in New York, including the annex buildings, and at offices away from Headquarters, based on a level of security infrastructure achieved through implementation of the approved projects for strengthening security and safety, taking into account the present or foreseeable threats and risks and bearing in mind the responsibilities and capacities of host Governments. The access control project is therefore intended to complement the considerable work already completed or under way at each main location for the enhancement of physical security and bring it to a consistent, modern, risk-managed and cost-effective standard, as determined by the Department of Safety and Security.

6. "Physical security" entails the full range of construction, fixtures, equipment and procedures that have as their collective purpose the denial of unwanted or criminal access to United Nations facilities. Those functional elements also provide for the safety and security, both routine and in an emergency, of persons authorized to be on United Nations premises. The standardized access control project complements, by bringing up to the necessary standards, those measures already approved by the General Assembly for strengthening the security and safety of United Nations premises both at Headquarters and at offices away from Headquarters. The proposed standardized access control project does not include the Secretariat complex at Headquarters, the requirements for which have been fully addressed through the projects on strengthening security and safety already approved by the General Assembly in its resolution 56/286 and being implemented by the capital master plan office. For Headquarters, the present report covers only the annex buildings, where a number of the Secretariat units as well as United Nations funds and programmes are located.

7. While host Governments bear the primary responsibility for the safety and security of United Nations personnel and activities, the Organization must retain security control within its property line, including access across it. The high symbolic status of each United Nations office at the main locations, including the International Tribunals, coupled with the significant number of staff members and associated personnel accommodated or visiting those locations, entails, depending on location, a medium to high level of risk. This necessitates the following access control functions: pass issuance and control, individual and vehicle access control, perimeter security monitoring, response to incidents and establishment and round-the-clock functioning of a security control centre at each location. These functions, which begin at the property line and continue through such additional layers of protection as may be required within the facility, are designed to channel personnel and vehicle access through control points for verification of identity and authority to

enter, as well as for other security checks. They must also provide for detection of and response to unauthorized entry attempts or other security breaches and for survivability and redundancy to ensure situational awareness and enable responders to react accordingly.

8. The global access control project, as set out by the Secretary-General (see A/59/365/Add.1 and Corr.1), entails system and information-sharing within and among all duty stations. The application of technology such as cameras, intrusion alarms and card-activated turnstiles or barriers, all of which are linked to a hardened local security command post, constitutes today's best practice for physical security at large office complexes at material risk. These modern systems lead to significant advantages in the comprehensiveness and reliability of access control, potentially allowing for more effective use of the security force for other duties such as close protection, investigations or quick response where the additional application of technology is either impracticable or not cost-effective. The potential implications, costs and benefits of linking locally integrated United Nations security systems into a global network, on the other hand, require further analysis.

B. Standardization and integration

9. Standardization, in the context of the proposed standardized access control project, entails "fitness for the purpose" as determined by the threats and risk level prevailing at each location, which is consistently monitored and validated by the Department of Safety and Security. In addition to complying with technical security standards and being compatible with equipment installed, the organizational processes and procedures for physical security must address life cycle cost-effectiveness at the specific locations concerned. There are potential economies of scale to be realized through systems contracts and the avoidance of duplication, coordinated training and unified procedures for system operation and maintenance as a result of standardization among as well as within the main locations.

10. The decision on security and safety standardization among the main locations will be taken in line with both the specific technical standards elaborated by the Department of Safety and Security and the detailed site-specific work at each main location in the course of the project design and engineering. Throughout the project and upon its operationalization, the project access control team will provide technical guidance to local security technicians on such issues as recommended procurement strategies, maintenance provisions, recommended maintenance programmes and operational procedures. The standardization will incorporate private and public sector security benchmarks for similar facilities; the selection of tried, tested and proven suppliers and technologies (taking into account survivability and redundancy); and technological "future-proofing". Should a decision be taken to procure a particular security system or device on a standardized local, regional or global basis, the team will also be responsible for developing uniform installation methodologies, maintenance provisions and recommended programmes as well as operational procedures that make the best use of existing infrastructure.

C. Management

11. The implementation of physical security measures is a shared responsibility of the Department of Safety and Security, the Department of Management and administrative services at each main location. In that connection, the Department of Safety and Security is responsible for providing technical security advice on the scope of work and ensuring that projects meet physical security standards and guidelines. The Department of Management will be responsible for the procurement, construction, financing and maintenance and support of the projects throughout their life cycles at New York, and the local administrative services will be responsible for the same functions at other main locations on the basis of the standard procedures and specifications governed by the Department of Safety and Security. The Department, through its Division of Headquarters Safety and Security Services, will operate the enhanced physical security regimes at each location once projects have been completed and are operational.

12. Site-specific plans that are tailored to local threats and risks and based on consistent standards are the key requirements for the cost-effective enhancement of physical security access control across all main locations. These requirements will be addressed through an enhanced management structure consisting of a steering group and the project access control team (see A/59/776). The steering group is led by the Under-Secretary-General for Safety and Security, with senior-level representation from the Department of Safety and Security and the Department of Management. The project access control team, as proposed by the Secretary-General (see A/59/776, para. 2), is composed of security specialists from the Department of Safety and Security and professionals from the Office of Central Support Services with expertise in information technology and facilities management.

13. Following the completion of initial field visits and a preliminary analysis of the requirements at all main locations, the project access control team will intensify its work in coordinating the more site-specific project definition as well as the implementation planning and support that lies ahead through the six-month process of detailed consultation. In order to ensure that the project is fully tailored to specific conditions on the ground, including arrangements with host Governments, threat assessments and joint security arrangements at each location will be regularly updated in coordination with local law enforcement and security authorities. With the support of the team, access control plans for each location will be verified in line with Department of Safety and Security standards. Care will be taken to ensure that those responsible for on-site procurement and implementation will receive the necessary technical security advice, guidance and assistance in all dimensions.

III. Outcome of assessment of the present security infrastructure at the main locations of the Organization

14. During 2005 the Department of Safety and Security, through a team of experts, undertook a comprehensive assessment of the security posture at each of the eight main locations of the Secretariat and at the International Tribunal for the Former Yugoslavia and the International Criminal Tribunal for Rwanda. The expert team was composed of members with knowledge of both industry and public sector best practices as well as of United Nations security practices at its main locations. In

accordance with the workplan for standardized access control proposed by the Secretary-General (ibid., para. 3) and with a view to providing technical assistance, the team was also accompanied by the project access control team technical consultant who in parallel has been reviewing background documentation related to the project. Information technology and facilities management experts, as well as security personnel, were consulted at each location in the course of the comprehensive assessment. Those visits were the first opportunity for the Department of Safety and Security to augment earlier reports with a comprehensive on-site survey of all the locations mentioned.

15. The experts noted that substantial security improvements had been implemented in the context of a large number of ongoing security and safety strengthening projects over the past two years. No redundant or overly designed projects in excess of requirements, as determined by local conditions, were identified by the experts. However, the team noted some delays in project implementation as well as shortfalls at some locations in connection with security coverage or in the technical parameters of particular barriers, perimeter surveillance or other access control measures. The team attributed these shortcomings in part to insufficient security capacity due to a lack of project management capacity and in part to a delay on the ground in recruitment against authorized security posts at the Professional level. The team, together with the project access control team technical consultant, has also identified specific instances at some locations where technical measures, either in place or planned, required upgrading or adjustment.

16. In its findings, the team of experts proposed that the various sets of minimum operating security standards currently in use, including the headquarters minimum operating security standards, be consolidated by the Department of Safety and Security into a single set of operational instructions that would incorporate additional details, while adding flexibility by setting out mandatory as well as advisory requirements. The team has further suggested that all locations should benefit from access to centralized technical support and guidance from security experts to be set up within the Department in the form of a small technical resource unit. In that regard, the Department, as a first step, would give top priority to the enhancement of security risk assessment procedures and to developing its physical security standards so as to guide ongoing implementation and the identification of future requirements across the United Nations and possibly providing guidance on procedures and standards to other organizations of the United Nations system. The Department, through the project access control team, would at the same time provide local managers with technical advice on a case-by-case basis so as to impart the appropriate security standards while avoiding unnecessary delays in the implementation of projects already under way.

17. The essential features for standardized access control at each main location are perimeter fencing and intrusion detection, rated personnel and vehicle barriers at access points, a reliable pass and identification card system, an operational command and control centre and closed-circuit television coverage at main points. In that connection, and taking into consideration the security strengthening projects either completed or at some stage of implementation, the team of experts and the project access control team, in close collaboration with the chiefs of security at each main location, have identified a number of specific additional requirements that should be addressed without delay. These urgent measures are to bring all surveyed locations to a baseline security level with regard to access control. They include

enhanced or additional vehicle barriers, upgraded perimeter coverage, reinforced security command posts and the introduction or extension of internal zoning. The project access control team has also identified instances in which the introduction or upgrading of locally integrated detection and access control technologies, such as additional closed-circuit television cameras, could present cost-effective opportunities for addressing physical security shortfalls. The additional financial requirements for this immediate physical enhancement of access control are estimated at $23,683,000, as set out in the table below.

Estimated resource requirements by duty station and function/project

(Thousands of United States dollars)

Duty station	*Perimeter intrusion*	*Closed-circuit television*	*Access control barriers*	*Identification server and badging stations*	*Security control room*	*Total*
Geneva	150.0	150.0	—	675.0	946.6	1 921.6
Vienna	210.0	100.0	176.6	525.0	1 100.0	2 111.6
Nairobi	—	1 862.9	2 200.0	425.0	600.0	5 087.9
Addis Ababa	439.4	650.0	950.0	425.0	1 150.0	3 614.4[a]
Santiago	750.0	800.0	577.5	425.0	600.0	3 152.5
Bangkok	—	245.0	—	375.0	325.0	945.0
Beirut	100.0	325.0	1 250.0	375.0	125.0	2 175.0
International Tribunal for the Former Yugoslavia	100.0	—	950.0	325.0	125.0	1 500.0
International Criminal Tribunal for Rwanda	550.0	—	950.0	400.0	75.0	1 975.0
New York annex buildings[b]	—	—	—	—	—	1 200.0
Total	**2 299.4**	**4 132.9**	**7 054.1**	**3 950.0**	**5 046.6**	**23 683.0**[b]

[a] In addition, estimated requirements in the amount of $417,300 for the access control system to be installed in the new office building at the Economic Commission for Africa (see A/60/532, para. 19) would be needed at a later stage. Those requirements will be included in the detailed implementation plan and cost estimates for the project, discussed in section V below.

[b] Urgent security measures for UNITAR, FF and Falchi (archives storage) buildings.

IV. Other considerations

A. Global identity management system

18. By section XI, paragraph 44 (e), of its resolution 59/276, the General Assembly requested detailed information regarding the global identity management system, including the principles and guidelines for sharing the information obtained

through the system, the level of centralization needed for managing the information and who would have access to the information. The global access control system, as proposed by the Secretary-General (see A/59/365/Add.1 and Corr.1), included a global identity management concept. This component of the project was intended to provide accurate identity data repositories, integrated exchange of identity data among all duty stations and databases and enhanced management of identity-related processes through the use of a central worldwide database.

19. The concept for standardized access control as set out in the present report entails the initial use of identity databases at the local level. In line with the Secretary-General's information and communication technology strategy (see A/57/620) and his bulletin on the use of information and communication technology resources and data (ST/SGB/2004/15), the access to, possession of or distribution of such sensitive data will be in accordance with all applicable United Nations regulations, rules and administrative issuances. The policy further establishes norms for safeguarding data and for staff accountability so as to preserve the confidentiality of the information. Access to identity information, in particular records relating to entering and exiting a facility, is deemed confidential and vital and therefore limited to those with a need to know. Local recording of such information, in line with current industry best practices for similar facilities, would be for the sole purpose of issuing passes and providing in an emergency a list of those persons present in the facilities. The data involved in this system, which supplants the need for manual records at entry and exit points, would not be used for any other purpose. The Department of Safety and Security, through the project access control team, will monitor closely the design and implementation of the identity management system at each main location. The Office of Internal Oversight Services, in accordance with Secretary-General's bulletin ST/SGB/2004/15, will also have authority to review and when necessary to conduct investigations into the access, use and sharing of identity data and processes.

20. As a first step, emphasis with respect to identity management will be placed on ensuring at each location a locally based pass issuance and control system of the required standard. In that connection, the Department of Safety and Security will issue and monitor common guidelines for the validation of identity documents, the maintenance of identity and access records and the application of security safeguards with respect to personal identity data to be incorporated into the design, issuance and withdrawal of identity cards or passes. A decision on linking local identity management into a global system will represent a possible further step should subsequent analysis identify a significant operational or cost-benefit advantage of linking local arrangements into a global identity management system. In that case the matter will be referred to the General Assembly for its decision with a full explanation of the rationale, the systems and database architecture involved and associated procedures for the sharing and protection of identity data.

B. Integration with the overall United Nations information technology strategy

21. In paragraph 44 (a) of section XI of its resolution 59/276, the General Assembly mandated the integration of the standardized access control system with other projects approved by the Assembly in previous resolutions, including those being implemented in the context of the overall information technology strategy. Information technology security, disaster recovery, business continuity and crisis

management are broader issues that, while outside the scope of the standardized access control project, may have an impact on this project by imposing new requirements for data links or technological applications. The Department of Safety and Security will therefore continue to maintain close coordination with the Information Technology Services Division of the Office of Central Support Services so as to ensure the compliance of ongoing, intended or future access control and other security activities or systems with the overall United Nations information technology strategy.

C. Impact on human resources requirements

22. In paragraph 44 (b) of section XI of its resolution 59/276, the General Assembly requested an assessment of the impact of implementing the global access control system on human resources requirements in the area of safety and security. As outlined previously in the present report, the introduction of access control technology presents opportunities to improve the quality of service by eliminating human error. It can also enable the more effective use of security personnel for other duties such as investigations, close protection or quick reaction forces through the reallocation of some security personnel to those functions. Specific decisions in that respect may be made at a later stage based on the experience gained from the functioning of the global access control system.

D. Implications for the capital master plan

23. In paragraph 44 (d) of section XI of its resolution 59/276, the General Assembly requested the Secretary-General to report on the implications of the global access control system for the capital master plan. It should be recalled that by its resolution 56/286, the General Assembly moved forward from the capital master plan the implementation of a complex-wide access control project at Headquarters, as proposed by the Secretary-General (see A/56/848, annex I, para. 40 (b) (ii), and annex II). The related measures included the reinforcement of perimeter protection and the installation of surveillance, monitoring and preventive measures linked to a security command centre. That project has been largely implemented. Given that the physical security requirements of the main Secretariat complex are fully addressed through the capital master plan project, the proposed standardized access control project in the case of Headquarters applies only to the Headquarters annex buildings. In that connection it should be noted that the capital master plan-managed project at the main Secretariat complex has been designed for full compatibility with the standardized access control project discussed in the present report.

V. Resource requirements for the project and time frame for implementation

24. It is foreseen that the implementation of the global access control project will be undertaken in two phases. During the first phase it is intended to rectify all shortcomings and gaps in physical security identified during the project reassessment process undertaken in 2005. Those requirements are detailed in paragraphs 14 to 17 above and in summary form in the accompanying table by duty station and function or project. The related costs are estimated at $23,683,000. It is

expected that these immediate improvements in physical security will be completed within a six-month period from the date of approval of this approach by the General Assembly through the temporary reprioritization of projects and utilization to the extent possible of resources approved under section 32, Construction, alteration, improvement and major maintenance, of the programme budget for the biennium 2006-2007 and in the budgets of the International Tribunals.

25. Subject to approval by the General Assembly of the proposed concept, scope and revised course of action for the project as reflected in the present report, during the first phase of project implementation it is also intended that a detailed definition of the project on a site-by-site basis would be developed and a detailed project implementation plan would be submitted to the Assembly at its sixty-first session. That plan would also include proposals for implementation of the project at the annex building at Headquarters, to be carried out on a cost-shared basis with the United Nations funds and programmes, the full project cost estimates and financing arrangements.

26. The second phase of project implementation would begin only after consideration of and approval by the General Assembly of the project proposals to be submitted to it at its sixty-first session. It is estimated that the second phase of implementation will take 18 to 24 months from the date of approval by the Assembly of the implementation plan and relevant financing arrangements.

VI. Conclusions and recommendations

27. **Following the review and assessment of the current status of access control at all main locations of the Organization, a two-phased approach for implementation of the standardized global access control system is proposed. In the first phase, during 2006, measures will be taken to rectify identified shortcomings and gaps in physical security at all main locations. The related estimated requirement in the amount of $23,683,000 is proposed to be met, to the extent possible, through the temporary reprioritization of projects approved for the current biennium under section 32, Construction, alteration, improvement and major maintenance, of the programme budget and in budgets of the International Tribunals.**

28. **Also during 2006, the Secretariat will prepare a detailed plan for implementation of the second phase of the project, addressing issues such as the optimum mixture, quantity, exact design specifications and procurement strategy for the project in all its main locations, defining the scope and approach for standardization and centralization at the local, regional and global levels, creating a capacity for technical security advice and support for system maintenance and identification of the impact of the global access control system on human resources requirements in the area of safety and security.**

29. **The detailed plan and estimated resource requirements for project implementation, including the replacement funding component with respect to measures to be implemented in 2006 in the context of the first phase of the project, will be submitted to the General Assembly at the main part of its sixty-first session.**

30. **The General Assembly is requested to approve the proposed course of action.**